3次体の3次不分岐巡回拡大の構成 (代数的整数論)

AUTHOR(S):

尾台, 喜孝

CITATION:

尾台, 喜孝. 3次体の3次不分岐巡回拡大の構成(代数的整数論). 数理解析研究所講究録 1986, 589: 136-148

ISSUE DATE:

1986-04

URL:

http://hdl.handle.net/2433/99430

数理解析研究所講究録
589巻 1986年 136-148

3次体の3次不分岐巡回拡大の構成

都立大・理　尾台　喜孝（Yoshitaka odai）

良く知られているように、2次体の2次不分岐拡大はGaussのgenus theoryによって容易に構成される。そこでここでは3次体の3次不分岐巡回拡大の構成について考察する。2次体の場合は2次不分岐拡大はすべてgenus fieldに含まれるので話が簡単に済んだ。3次体の場合でもgenus fieldに含まれる3次不分岐巡回拡大は構成方法が知られている。([2])しかしgenus fieldに含まれないものが存在するので、それらの構成が問題になる。この問題に対して、elementaryな方法である程度の結果を得たので以下に報告する。なお純3次体の場合については既に[4]に発表した。

記号

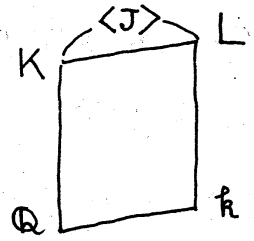
K：実3次体

$k = \mathbb{Q}(\zeta)$,　　$\zeta = \exp(2\pi i/3)$

$L = K\mathbb{R}$

$Gal(L/K) = \langle J \rangle$

J: complex conjugate mapping



§1. 3次体一般

Lemma A：Kの3次不分岐巡回拡大すべての集合.

B：Lの3次不分岐巡回拡大でK上abelなものすべての集合.

Bの元はKummer理論より. $L(\sqrt[3]{\alpha})$, $\alpha \in L^{\times}$ と書けるが、このとき写像

$$P : B \ni L(\sqrt[3]{\alpha}) \longrightarrow K(\mathrm{Re}\sqrt[3]{\alpha})$$ $\mathrm{Re}*$：*の実部

はBからAの上への全単射になる。

Proof. $L(\sqrt[3]{\alpha})$に$L(\sqrt[3]{\alpha})/K$の3次中間体を対応させる写像がBからAの上への全単射になることはすぐわかる。従って、$[K(\mathrm{Re}\sqrt[3]{\alpha}) : K] = 3$を示せばよい。

$L(\sqrt[3]{\alpha})/K$ abel $\Rightarrow \alpha^{1+J} \in (L^{\times})^3 \Rightarrow (\sqrt[3]{\alpha})^{1+J} \in L \cap \mathbb{R} = K$

よって、$\sqrt[3]{\alpha} + \sqrt[3]{\alpha}^{J} = 2\,\mathrm{Re}\sqrt[3]{\alpha}$ に注意すれば、$\sqrt[3]{\alpha}$ は$K(\mathrm{Re}\sqrt[3]{\alpha})$上2次。これより$[K(\mathrm{Re}\sqrt[3]{\alpha}) : K] = 3$が従う。

Theorem 1　Kの3次不分岐巡回拡大はKに$\mathrm{Re}\sqrt[3]{\alpha}$を添加

して得られる。但しαは次の条件を満たす$L^\times$の元：

0. $\alpha \notin (L^\times)^3$

I. (i) αはイデアルとして立方

(ii) αは$\mathrm{mod}(1-\zeta)^3$で立方剰余

II. $\alpha^{1+J} \in (L^\times)^3$

Proof. Lemmaより$\mathbb{B}$を求めればよい。$\mathbb{B}$の元の条件をKummer拡大の理論で書き直せば条件0~IIになる。

これでKの3次不分岐巡回拡大を構成することは、$L^\times$の元で条件0～IIを満たすものを捜すことに帰着された。

Remark 1　αは$L^\times/(L^\times)^3$の元と思ってよい。

☺ $\alpha' = \alpha\beta^3 \Rightarrow L(\sqrt[3]{\alpha}) = L(\sqrt[3]{\alpha'}) \Rightarrow K(\sqrt[3]{\alpha}) = K(\sqrt[3]{\alpha'})$。

Remark 2　$H := \{ \mathfrak{h} : L\text{のイデアル類} \mid \mathfrak{h}^3 = 1 \}$

明らかに．　αがI(i)を満たす $\Leftrightarrow (\alpha) = \mathfrak{a}^3$, $\mathfrak{a} \in \mathfrak{h} \in H$

これよりHとLの単数群E_LがわかればI(i)を満たすαがわかる。しかもHとE_L/E_L^3は有限ゆえ、そういうαは有限個。

Remark 3　$H^- := \{ \mathfrak{h} \in H \mid \mathfrak{h}^J = \mathfrak{h}^{-1} \}$

すると，　αがI(i), IIを満たす $\Rightarrow (\alpha) = \mathfrak{a}^3$, $\mathfrak{a} \in \mathfrak{h} \in H^-$

☺ $\alpha^{1+J} \in (L^\times)^3 \Rightarrow \mathfrak{a}^{1+J}$が単項 $\Rightarrow \mathfrak{h}^{1+J} = 1$。

§2. 巡回3次体及び純3次体の場合

まず純3次体の定義：

$$K\text{が純3次体} \iff K=\mathbb{Q}(\sqrt[3]{m}),\ \exists m\in\mathbb{Z}$$

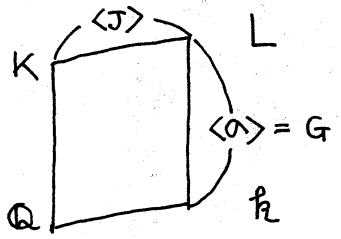
3次体に関して次の事実は良く知られている：

$$L/k\text{が巡回拡大} \iff K\text{が巡回3次体又は純3次体}$$

以下この§では，Kは巡回3次体又は純3次体と仮定する。

$G=\mathrm{Gal}(L/k)$

σ：Gの生成元



Theorem 2　M：Kのgenus field（i.e. Kの絶対類体の最大絶対アーベル部分体とKとの合成体）

Kの3次不分岐巡回拡大$K(\sqrt[3]{\alpha})$がMに含まれないための必要十分条件は．

$$\text{III.}\quad \alpha^{\sigma-1}\notin (L^{\times})^3$$

Proof. genus fieldの定義とガロア群の群論的考察により．

$$K(\sqrt[3]{\alpha})\subset M \iff L(\sqrt[3]{\alpha})/k \quad \text{abel}$$

Kummer拡大の理論より．　$L(\sqrt[3]{\alpha})/k$ abel $\iff \alpha^{\sigma-1}\in(L^{\times})^3$

さて、§1のRemark 2で注意したように

$$H = \{ \mathfrak{h} : L\text{のイデアル類} \mid \mathfrak{h}^3 = 1 \}$$

が問題になる。$\mathcal{H}$をLのイデアル類群の3-Sylow subgroupとする。$\mathcal{H}$は$\mathbb{Z}[G]$-module ゆえ

$$\mathcal{H}_i := \{ \mathfrak{h} \in \mathcal{H} \mid \mathfrak{h}^{(\sigma-1)^i} = 1 \} \qquad i \in \mathbb{N} \cup \{0\}$$

が定義できる。$\mathfrak{h}$の類数が1であることより

$$\begin{array}{l} \mathcal{H}_2 = H \\ \cup \\ \mathcal{H}_1 : \mathfrak{h}\text{に関する特異類群} \\ \cup \\ \mathcal{H}_0 = \{1\} \end{array}$$

が証明される。

さらに$i = 0, 1, 2$に対して

F_i：Kの3次不分岐巡回拡大で，$\mathcal{H}_i$ からつくられるものすべての合成体。

但し，“$\mathcal{H}_i$からつくられる”とは，Th 1のαが

$(\alpha) = \mathfrak{a}^3$, $\mathfrak{a} \in \mathfrak{h} \in \mathcal{H}_i$ なるときにいう。

と定義する。すると、§1のRemark 2より

$$\begin{array}{l} F_2 : K\text{の3次不分岐巡回拡大すべての合成体} \\ \cup \\ F_1 \\ \cup \\ F_0 : \alpha \in E_L \text{ なるものすべての合成体} \end{array}$$

となる。

また、Lの$\mathfrak{k}$に関する特異イデアルを含む類のなす群を$\mathcal{H}_1^0$と書き、F_1^0をF_iと同様に定義する。

$$\mathcal{H}_0 \subset \mathcal{H}_1^0 \subset \mathcal{H}_1, \quad F_0 \subset F_1^0 \subset F_1 .$$

Grasにより$\mathcal{H}_2$を求めるアルゴリズムが得られている。([1])しかし、実行するには途中のNorm方程式の部分がかなり大変である。そこで、ここではF_2はあきらめて、F_0, F_1^0, F_1について考察する。

Proposition 3　M：Kのgenus field

$$F_1^0 = F_0 M$$

さらに，－partを§1. Remark 3のように定義すれば、

$$\mathcal{H}_1^- = \mathcal{H}_1^{0-} \Rightarrow F_1 = F_0 M$$

Proof（概略）

$P_1, \cdots P_s, q_1, \cdots q_t$：Kで分岐する有理素数，$P_i \equiv 1$, $q_i \equiv -1 \bmod 3$

$P_i = \pi_i^{1+J}$　　π_i：$\mathfrak{k}$の素元，$\equiv 1 \bmod 3$

$\pi = \sqrt{-3}$ if L/$\mathfrak{k}$で$(\sqrt{-3})$が分岐

すると、π_i, π_i^J, q_i, πがL/$\mathfrak{k}$で分岐する$\mathfrak{k}$のprime全部。

1st step. $M = K\left(\mathfrak{k}\sqrt[3]{\pi_i^{1+2J}} \mid i=1,\cdots,s\right)$ を証明する。

2nd step. $\mathcal{H}_1^0$がLの$\mathfrak{k}$上分岐する素イデアルを含む類のなす群と一致することを証明する。

3rd step　§1. Remark 3よりF_1^0を求めるには

$$(\alpha) = \mathfrak{a}^3,\ \mathfrak{a} \in \mathfrak{h} \in \mathcal{H}_1^{0-}$$

なるαを考えればよい。（よって、$\mathcal{H}_1^- = \mathcal{H}_1^{0-} \Rightarrow F_1 = F_1^0$）

すると2nd stepの結果より

$$\alpha = \varepsilon \prod \pi_i^{a_i+b_iJ} \cdot \prod \mathfrak{q}_j^{c_j} \cdot \pi^d,\quad \varepsilon \in E_L,\ a_i, b_i, c_j, d \in \mathbb{Z}/3\mathbb{Z}$$

さらに条件IIを満たすためには、$b_i = 2a_i$, $c_j = d = 0$。

$$\therefore \alpha = \varepsilon \prod (\pi_i^{1+2J})^{a_i}$$

1st stepの結果と比べてProp.を得る。

<u>Corollary</u>　Kが巡回3次体のとき、導手を$\mathfrak{m}$とする。

$\mathfrak{m}$が(1)または(2)を満たせば　$F_1 = F_0M$

(1) $\exists p$: prime　s.t. $p \mid \mathfrak{m}$, $p \neq 3$, $p \not\equiv 1 \bmod 9$

(2) $\mathfrak{m} = \mathfrak{q}$

Kが純3次体のときは常に　$F_1 = F_0M$

<u>Proof.</u>　$A = \mathcal{H}_1/\mathcal{H}_1^0$,　$B = (E_k \cap N_{L/k}L^\times)/N_{L/k}E_L$

$A^\pm := \{\mathfrak{h} \in A \mid \mathfrak{h}^J = \mathfrak{h}^{\pm 1}\}$, $B^\pm$も同様に定義。（複号同順）

$A \ni \mathfrak{h}$に対し、$\mathfrak{h} \ni \mathfrak{a}$, $\mathfrak{a}^{\sigma-1} = (\alpha)$, $N_{L/k}\alpha = \varepsilon$で決まる$\varepsilon$を対応させることにより$A \cong B$となる。Kが巡回のときは$\sigma J = J\sigma$ ゆえ$A^- \cong B^-$。よって、$A^- = \{1\} \Leftrightarrow B^- = \{1\} \Leftrightarrow \zeta \notin N_{L/k}L^\times$ $\Leftrightarrow$ $\mathfrak{m}$が(1)または(2)を満たす。Kが純のときは$\sigma J = J\sigma^2$ゆえ$A^- \cong B^+$。よって、$A^- = \{1\} \Leftrightarrow B^+ = \{1\}$。これは常にO.K..

従ってProp.3よりCor.が証明される。

Remark. 講演ではKが巡回3次体のときも含めて常に$F_1 = F_0 M$であると述べたが、それは言い過ぎだった。現在証明できているのはCor.まで。

Prop.3より、F_0, 特にF_0のうちMに含まれない部分が問題になる。すなわちE_Lの元で条件0～III (Th2) を満たすものが問題になる。巡回3次体と純3次体に分けて考察する。

E_*：＊の単数群,　　W_*：＊の1の根の群

巡回3次体　Lは虚巡回体ゆえ

$$E_L = E_k W_L = E_k W_k \quad \text{if } K\text{の導手} \neq 9$$

$W_k^{1+\sigma} = W_k^{\sigma-1} = 1$に注意すれば、$E_L$の元でIIとIIIを同時に満たすものが存在しないことがわかる。

$$\therefore F_0 \subset M \quad (K\text{の導手が}9\text{のときも}K = F_0 = M)$$

純3次体　([4])　e：Kの基本単数でnormが1のもの。$X^{1-\sigma} = e$がE_L内で解を持たないときをCase 1, 持つときをCase 2, そのときの解の1つをεとする。

Case 1.　Lの基本単数系として$\{e, e^\sigma\}$がとれる。従って、$\zeta^a e^{b+c\sigma}$ $(a, b, c \in \mathbb{Z}/3\mathbb{Z})$について条件をみればよい。$J\sigma = \sigma^2 J$, $e^J = e$, $e^{\sigma^2} = e^{-1-\sigma}$ に注意して計算してみると、IIとIIIを同時に満たすものは存在しない。

$\therefore F_0 \subset M$

Case 2. L の基本単数系として $\{\varepsilon, \varepsilon^\sigma\}$ がとれる。$\varepsilon^{1-\sigma} = e$ より $\varepsilon^J = \pm\varepsilon^{-\sigma}$ がわかるので、これと $\varepsilon^{\sigma^2} = \varepsilon^{-1-\sigma}\eta$ ($\eta \in W_k$) に注意して計算してみると、$\zeta^a\varepsilon^{1+\sigma}$ だけがⅡとⅢを同時に満たす。(もちろん O, I(i) も満たす。) I(ii) の判定は局所体の中での素元による展開を用いて容易にできる。特にこれは I(ii) を満たさないので、$\zeta^a\varepsilon^{1+\sigma}$ のうち I(ii) を満たすのはせいぜい1個

以上まとめて:

Theorem 4 K が巡回3次体: $F_1^0 = M$

導手 $\mathfrak{m}$ が Cor. の条件を満たせば、 $F_1 = M$

K が純3次体: Case 1, 2, ε を上と同じとする。

Case 1. $F_1 = M$

Case 2. $U := \{\zeta^a\varepsilon^{1+\sigma}\ (a=0,1,2)$ のうち I(ii) を満たすもの$\}$

$\#U \leqq 1$, $\begin{cases} U = \phi \Rightarrow F_1 = M \\ U = \{\varepsilon_0\} \Rightarrow F_1 = M(\sqrt[3]{\varepsilon_0}) \neq M \end{cases}$

例

$K = \mathbb{Q}(\sqrt[3]{m})$ $m \in \mathbb{Z}$, >0, cube free

(*) $m = D^3 + d$, $D, d \in \mathbb{Z}$, $D > 0$, $d \mid 3D^2$

$$(D,d)\neq(1,1),(2,1),(1,3),(2,-6),(5,-25),(2,-4)$$

とすると、

$$\begin{cases} d=\pm1 \Rightarrow \text{Case 1} \\ d\neq\pm1 \Rightarrow \text{Case 2}\ ,\ \varepsilon=(\sqrt[3]{m}-D)^{1-\sigma^2} \end{cases}$$

I(ii)の判定を行なって次のProp.を得る：

Proposition 5 ([4]) Kが純3次体で(♯)を満たしていて，さらに$d\neq\pm1$とする。$\varepsilon=(\sqrt[3]{m}-D)^{1-\sigma^2}$とおく。このとき Th.4のひは次のようになる：

	$3\nmid m$	$3\parallel m$	$3^2\parallel m$
$3\nmid D$	$*_{(1)}$	ϕ	$*_{(2)}$
$3\parallel D$	$\{\zeta\varepsilon^{1+\sigma}\}$	$*_{(3)}$	ϕ
$3^2\mid D$	$\{\zeta\varepsilon^{1+\sigma}\}$		

(1)

m	$3\nmid d$	$3\mid d$
$\pm1 \bmod 3^2$	ϕ	ϕ
±2 〃	$\{\varepsilon^{1+\sigma}\}$	
±4 〃	$\{\zeta\varepsilon^{1+\sigma}\}$	

(2) $\begin{cases} m/3^2\equiv D \bmod 3 \Rightarrow \{\zeta^2\varepsilon^{1+\sigma}\} \\ m/3^2\equiv -D \bmod 3 \Rightarrow \{\zeta\varepsilon^{1+\sigma}\} \end{cases}$

(3) $\begin{cases} m/3\equiv D/3 \bmod 3 \Rightarrow \{\zeta^2\varepsilon^{1+\sigma}\} \\ m/3\equiv -D/3 \bmod 3 \Rightarrow \{\varepsilon^{1+\sigma}\} \end{cases}$

Remark このProp.より，genus fieldに含まれない3次不分岐巡回拡大を構成できる3次体の例が無限個得られる。

数値例 (1) Prop.5 に属する例。$U \neq \emptyset$ なるもの：

m	30	68	130	204	210
D	3	4	5	6	6
d	3	4	5	−12	−6
U	$\{\zeta^2\varepsilon^{1+a}\}$	$\{\zeta\varepsilon^{1+a}\}$	$\{\zeta\varepsilon^{1+a}\}$	$\{\zeta^2\varepsilon^{1+a}\}$	$\{\varepsilon^{1+a}\}$

(2) Prop.5 に属さない例。

$m = 34$ $\quad \varepsilon = 305 + 94\sqrt[3]{34} + 29\sqrt[3]{34}^2 - 52\zeta - 16\sqrt[3]{34}\zeta - 5\sqrt[3]{34}^2\zeta$

$U = \{\varepsilon^{1+a}\}$

§3. 巡回3次体でも純3次体でもない場合

最後に、講演では触れることができなかったが、Kが巡回3次体でも純3次体でもない場合について述べる。この場合§2の最初で述べたように、L/k は Galois 拡大にならず、§2の議論は成り立たない。ここでは小規模な変更で対応する結果が得られる部分について報告する。証明方法は主張を見ればだいたい想像がつくと思うので省略する。

まず、Th.2に対応する結果：

Theorem 2′ D_K：Kの判別式，$\hat{L} = L(\sqrt{D_K})$，$\hat{k} = k(\sqrt{D_K})$，

の：$\mathrm{Gal}(\tilde{L}/\tilde{K})$ の生成元。Kの3次不分岐巡回拡大 $K(\sqrt[3]{\alpha})$ がgenus field Mに含まれないための必要十分条件は，

$$\text{Ⅲ}'.\quad \alpha^{\sigma-1} \notin (\tilde{L}^{\times})^3$$

$\mathcal{H}_i$, $\mathcal{H}_i^0$, F_i, F_i^0 は§2のように定義することはできないが、$\mathcal{H}_0 := \{1\}$ と定義すれば F_0 は定義できる。

Theorem 4′ Kが総実：$F_0 \subset M$

Kが非総実：$\{u \in E_L \mid N_{L/K}(u) = \pm 1\} = W_L \cdot \langle \varepsilon \rangle$ なる ε が存在する。ε が条件Ⅲ′を満たさないときをCase 1，満たすときをCase 2とする。

Case 1. $F_0 \subset M$

Case 2. $U := \{ \zeta^a \varepsilon \ (a=0,1,2)$ のうちI(ii)を満たすもの $\}$

$$\begin{cases} U = \phi & \Rightarrow \quad F_0 \subset M \\ U \ni \varepsilon_0 & \Rightarrow \quad F_0 \not\subset M,\ F_0 \subset M(\sqrt[3]{\alpha}) \end{cases}$$

Remark ε を求め，同時に ε がⅢ′を満たすかどうかの判定をするアルゴリズムが得られている。([3])

例 Prop.5のような系列例は得られていないが，[3]のアルゴリズムを，コンピューターを用いて実行することによっ

て次の例が得られた。

$K = \mathbb{Q}(\theta)$　　$\theta : X^3 - 6X^2 + 24X - 12 = 0$ の実根.

$\varepsilon : X^3 - 3(-27+55\zeta)X^2 + 3(-82-55\zeta)X - 1 = 0$ の絶対値1の根.

$\zeta^2\varepsilon \in U$

参考文献

[1] G.Gras, Sur les ℓ-classes d'ideaux dans les extensions cycliques relatives de degré premier ℓ, Ann. Inst. Fourier 23, 3, (1973), 1-48, 23,4, (1973), 1-44.

[2] M. Ishida, The genus fields of algebraic number fields, Lecture Notes in Math., 555, Springer, Berlin-Heiderberg-New York, 1976.

[3] K.Nakamula, Class number calculation of a sextic field from the elliptic unit, Acta Arith. XLV (1985), 229-247.

[4] Y. Odai, Some unramified cyclic cubic extensions of pure cubic fields, Tokyo J. Math. 7, (1984), 391-398.